引用例２の対応国際公開公報の写し

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06K 19/073 — A1

(11) International Publication Number: **WO 95/19608**

(43) International Publication Date: 20 July 1995 (20.07.95)

(21) International Application Number: PCT/IB95/00032

(22) International Filing Date: 13 January 1995 (13.01.95)

(30) Priority Data:
08/181,684 14 January 1994 (14.01.94) US

(71) Applicant: BULL CP8 [FR/FR]; 68, route de Versailles, Boîte postale 45, F-78430 Louveciennes (FR).

(72) Inventor: HOLTEY, Thomas, O.; 10 Crehore Drive, Newton, MA 02162 (US).

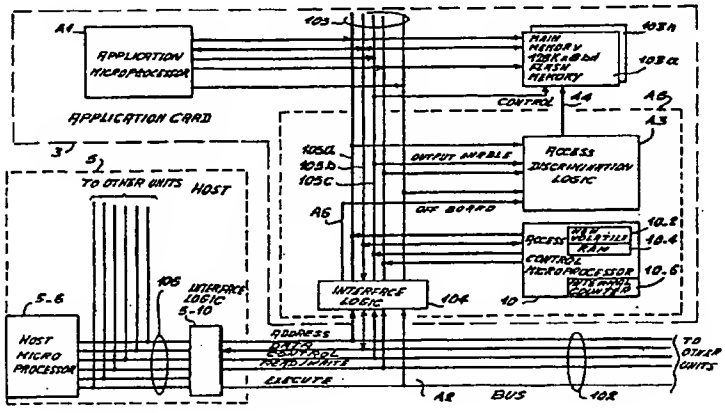
(74) Agent: CORLU, Bernard; Bull S.A., 68, route de Versailles, Boîte postale 45, F-78430 Louveciennes (FR).

(81) Designated States: CA, CN, FI, JP, KR, NO, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

BEST AVAILABLE COPY

(54) Title: A SECURE APPLICATION CARD FOR SHARING APPLICATION DATA AND PROCEDURES AMONG A PLURALITY OF MICROPROCESSORS



(57) Abstract

A secure application memory card (3) can be operatively connected with a host microprocessor (5-6) via a standard interface, and contains an access control microprocessor (ACP 10) on a single semiconductor chip which interconnects to a number of non-volatile addressable memory chips (103a, 103n) each organized into a plurality of blocks. The microprocessor includes an addressable non-volatile memory (10-2) for storing information including a number of key values and program instruction information and security control unit for protecting the data contents of the non-volatile memory chips from unauthorized access. The memory card futher includes an application processor (A1) and an access discrimination logic unit (A3). The access discrimination logic unit includes an access by type memory writable by the application processor (A1) under the control of the ACP (10) for maintaining security. The memory has a plurality of locations, each location having a plurality of access control bits and being associated with a different block of the non-volatile memory chip for defining the different types of access permitted to such block.

【한국공개특허공보 1996-701414호(1996.02.24) 1부.】

引用例２の写し

(19) 대한민국특허청(KR)
(12) 국제특허출원의 출원공개공보(A)

(51) Int. Cl.[6]
G06K 19/073

(11) 공개번호 특1996-7001414
(43) 공개일자 1996년02월24일

(21) 출원번호 특1995-7003947
(22) 출원일자 1995년09월14일
번역문제출일자 1995년09월14일
(86) 국제출원번호 PCT/IB 95/000032 (87) 국제공개번호 WO 95/019608
(86) 국제출원출원일자 1995년01월13일 (87) 국제공개일자 1995년07월20일
(81) 지정국 EP 유럽특허 : 오스트리아 벨기에 스위스 리히텐슈타인 서독 덴마크 스페인 불란서 영국 그리이스 아일랜드 이태리 룩셈부르크 모나코 네덜란드 포르투갈 스웨덴
국내특허 : 캐나다 중국 핀란드 일본 한국 노르웨이
(30) 우선권주장 8/181,684 1994년01월14일 미국(US)
(71) 출원인 쎄뻬8 트랜색 미쉘 꼴롱브
프랑스공화국 78430 루브시엔느 베.뻬. 45 루트 드 베르사이유 68
(72) 발명자 토마스 오. 홀티
미합중국 매사츄셋츠 02162 뉴톤 크레호어 드라이브 10
(74) 대리인 이병문, 이태희

심사청구 : 있음

(54) 복수의 마이크로 프로세서들간에 애플리케이션 데이터 및 절차들을 공유하기 위한 보안성 애플리케이션 카드

요약

보안 애플리케이션 메모리 카드(3)는 표준 인터페이스를 통해 호스트 마이크로 프로세서(5-6)에 동작가능하게 접속될수 있고, 다수의 블럭들로 구성된 다수의 어드레스 가능한 비 휘발성 메모리 칩들(103a,103n)에 상호접속하는 단일 반도체 칩상에 액세스 제어 마이크로 프로세서(ACP 10)을 포함한다. 상기 마이크로 프로세서는 다수의 키의 값들 및 프로그램 교육 정보를 저장하는 어드레서가능한 비 휘발서 메모리(10-2) 및 허가받지 않은 애겟스로부터 비 휘발서 메모리 칩들의 데이터 내용을 보호하는 보안 제어 유닛을 포함한다. 상기 메모리 카드는 애프리케이션 프로세서(A1) 및 액세스 식별 논리 유닛(A3)을 더 포함한다. 상기 액세스 식별 논리 유닛은 보안을 유지하도록 ACP(10)의 제어하에 애플리케이션 프로세서(A1)에 의해 기입 가능한 타입의 메모리에 의한 액세스를 포함한다. 상기 메모리는 다수의 위치들을 가지며, 각 위치는 다수의 액세스 제어 비트를 가지며 상기 블럭에 허용되는 다른 타입의 액세스를 한정하도록 비 휘발성 메모리 칩의 다른 블럭과 관련된다.

대표도

도1

명세서

[발명의 명칭]

복수의 마이크로 프로세서들간에, 애플리케이션 데이터 및 절차들을 공유하기 위한 보안성 애플리케이션 카드

[도면의 간단한 설명]

제1도는 본 발명에 따라 구성된 애플리케이션 카드를 결합시킨 시스템의 블럭선이다,

제2도는 제1도에서의 플래시 메모리의 구조를 더욱 상세히 보인 도면이다,

제3도는 본 발명에 따라 구성된, 제1도에서의 액세스바이 타입 메모리를 더욱 상세히 보인 도면이다,

제4도는 본 발며의 애플리케이션 카드의 동작을 설명하기 위해 사용된 시스템 배열도이다.

본 내용은 요부공개 건이므로 전문 내용을 수록하지 않았음

(57) 청구의 범위

청구항 1. 버스 인터페이스를 통해 결합된 호스트 마이크로 프로세서와 조합되어 사용되는 애플리케이션 카드로서: 상기 호스트 마이크로 프로세서로의 그리고 그 호스트 마이크로 프로세서로부터의, 어드레

스, 데이터 및 제어 정보를 포함하는 요청들을 송수신하도록 상기 버스 인터페이스에 유효하게 결합된 인터페이스 논리회로 수단; 상기 인터페이스 논리회로 수단에 접속되며, 상기 인터페이스 논리회로 수단으로부터, 어떤 마이크로 프로세서가 상기 메모리 요청을 하는지 그리고 어떤 타입의메모리 액세스가 이루어지는지를 한정하는 각 메모리 요청에 관한 신호를 포함하는 요청을 전송하기 위한 어드레스, 데이터 및 제어부를 갖는 내부 버스; 상기 내부 버스에 접속되며, 특정 애플리케이션을 실행하도록 코드된 비 휘발성 메모리 매핑 정보를 포함하는 구성 정보를 저장하기 위한 어드레스 가능한 비 휘발성 메모리를 포함하는 액세스 제어 마이크로 프로세서; 상기 어드레스, 데이터 및 제어부에 결합되는 액세스 식별 논리 유닛으로서, 상기 애플리케이션 실행에 관계된 각 마이크로 프로세서 및 메모리 요청에 응답하는 상기 액세스 식별 논리 유닛에 의해 각 블럭에 대해 만들어지는 별개의 메모리 액세스 바이 타입 정보를 한정하도록 코드된 상기 다수의 블럭들을 위한 상기 비 휘발서 에모리 매핑 정보에 대응하는 액세스 바이 타입 정보를 저장하고, 상기 마이크로 프로세서가 상기 액세스 바이 타입 정보에 의해 한정된 상기 메모리 요청만에 의해 지정된 상기 블럭들 중 하나와 관계된 상기 액세스 바이 타입 정보를 판독하는 액세스 식별 논리 유닛을 포함하는 애플리케이션 카드.

청구항 2. 제1항에 있어서, 상기 액세스 식별 논리 유닛은; 상기 내부 버스의 어드레스, 데이터 및 제어부에 각각 접속된 어드레스, 데이터 및 제어입력, 상기 비 휘발성 메모리에 접속된 출력, 및 상기 비 휘발성 메모리 매핑 정보를 저장하기 위한 상기 갯수의 블럭들의 갯수에 대응하는 복수의 저장 위치들을 가진 랜덤 엑세스 에모리(RAM)어레이를 포함하며, 각 저장 위치는 상기 애플리케이션 실행에 요구되는 에모리 액세스 타입을 지정하기 위한 상기 에모리 매핑 정보에 의해 한정되는 소정 상태로 세트된 다수의 액세스 제어 비트 위치들을 가지며, 상기 RAM어레이는 각 에모리 요청에 응답하며 상기 어드레스 정보에 의해 지정된 상기 복수의 저장 위치들 중 하나에서의 메모리 매핑 정보를 판독하고, 상기 액세스를 인에이블하도록 하기 위한 상기 인터페이스 논리회로 수단으로부터의 상기 신호에 의해 한정된 상기 액세스 제어 비트 위치들 중 하나로부터의 상기 소정 상태들 중 하나에 대응하는 제어 신호로서 상기 출력에 인가하는 애플리케이션 카드.

청구항 3. 제1항에 있어서, 상기 액세스 제어 마이크로 프로세서 및 액세스 식별 논리 유닛이 단일 칩 내에 포함되는 애플리케이션 카드.

청구항 4. 제2항에 있어서, 상기 액세스 식별 논리 유닛은; 데이터 및 제어 입력 및 출력 회로 수단을 가진 멀티프렉서 셀렉터 회로 수단을 더 포함하며, 상기 데이터 입력들은 사기 에모리 매핑 정보를 수신하기 위해 상기 RAM어레이에 결합되며, 상기 제어 입력들은 상기 인터페이스 논리회로 수단 및 상기 비 휘발성 메모리에 결합된 상기 출력 회로 수단으로부터 상기 신호들을 수신하기 위한 상기 제어부에 결합되며, 상기 멀티플렉서 셀렉터 회로 수단은 상기 제어 입력들에 인가된 상기 신호들에 응답하며 상기 엑세스를 인에이블링 하기 위해 상기 출력 회로에 상기 제어신호를 인가하기 위한 상기 액세스 제어 비트 위치들 중 하나를 선택하는 애플리케이션 카드.

청구항 5. 제3항에 있어서, 상기 출력회로 수단은 적어도 제1 및 제2입력 및 출력을 가진 논리회로를 포함하며, 상기 제1입력은 상기 제어신호를 수신하도록 접속되며 상기 제2입력은 상기 제어부의 소정 버스라인에 접속되며 상기 출력은 상기 비 휘발성 메모리에 접속되며, 상기 신호들은 상기 에모리 요청을 발생시킨 마이크로 프로세서를 나타내는 오프 보드 신호 및 상기 에모리 액세스의 타입을 한정하는 버스 액세스 제어 신호를 포함하는 애플리케이션 카드.

청구항 6. 제5항에 있어서, 상기 버스 액세스 제어 신호는 상기 액세스를 요청한 마이크로 프로세서가 액세스되고 있는 상기 블럭내의 정보만을 실행할 수 있게끔 한정하기 위해 코드된 실행 제어 신호인 애플리케이션 카드.

청구항 7. 제5항에 있어서, 상기 버스 액세스 제어 신호는 액세스를 요청한 마이크로 프로세서가 액세스 되고 있는 상기 블럭내의 정보를 판독하여 실행할 수 있게끔 한정하기 위해 코드된 판독 제어 신호인 애플리케이션 카드.

청구항 8. 제3항에 있어서, 상기 비 휘발성 에모리의 상기 블럭들 중 제1그룹이 상기 애플리케이션에 관계하는 제1타입의 데이터를 저장하며 상기 블럭들의 상기 제1그룹중 다른 하나와 관계된 각 저장 위치의 제1액 제어비트 위치는 상기 특정 애플리케이션을 실행하기 위한 동작을 실행하도록 프로그램된 애플리케이션 마이크로 프로세서에 의해 상기 블럭들의 제1그룹내의 저장위치들로 액세스를 인에이블 하도록 하기 위한 제1상태로 세트되며 상기 각 저장 위치의 제2액세스 제어 비트 위치는 상기 데이터를 액세스하도록 인가되지 않은 호스트 마이크로 프로세서에 의해 상기 블럭들의 제1그룹내의 저장위치들로의 액세스가 금지되게 하기 위한 제2상태로 세트되는 애플리케이션 카드.

청구항 9. 제8항에 있어서, 사기 제1 및 제2상태는 각각 2진의 ONE 및 2진의 ZERO에 대응하는 애플리케이션 카드.

청구항 10. 제8항에 있어서, 상기 비 휘발성 에모리의 상기 블럭들의 제2그룹이 상기 애플리케이션에 관계하는 제2타입의 데이터를 저장하며 상기 블럭들의 상기 제2그룹 중 다른 하나와 관계된 각 저장 위치의 상기 제1액세스 제어 비트 위치는 상기 애플리케이션 마이크로 프로세서에 의해 상기 블럭들의 상기 제2그룹내의 저장 위치들로의 액세스를 금지하도록 하기 위한 상기 제2상태로 세트되며 상기 각 저장 위치의 상기 제2액세스 제어 비트 위치는 상기 호스트 마이크로 프로세서에 의해 상기 제2그룹의 위치들내의 저장위치들로 액세스를 인에이블 하게 하는 상기 제1상태로 세트되는 애플리케이션 카드.

청구항 11. 제10항에 있어서, 상기 비 휘발서 에모리의 상기 블럭들의 제3그룹은 상기 애프리케이션에 관계되는 동작의 실행시에 상기 애플리케이션 마이크로 프로세서에 의해 사용되는 제1타입의 프로그램 정보를 저장하며 상기 블럭들의 제3그룹 중 다른 하나와 관계된 각 저장위치의 제3액세스 제어 비트 위치는 상기 특정 애플리케이션을 실행하기 위한 동작을 실행하도록 프로그램된 애플리케이션 마이크로 프로세서에 의해 상기 블럭들의 제1그룹내의 저장위치들로 액세스를 인에이블 하게 하기 위한 제1상태로 세트되며 상기 각 저장위치의 제4액세스 제어 비트 위치는 보안을 유지하기 위해 상기 프로그램 정보를 액세스하도록 인가되지 않은 호스트 마이크로 프로세서에 의해 상기 블럭들의 제3그룹내의 저장위치들로의 액세스를

금지하도록 하기 위한 상기 제2상태로 세트되는 애플리케이션 카드.

청구항 12. 제11항에 있어서, 상기 비 휘발성 메모리의 상기 블럭들 중 제4그룹이 상기 애플리케이션에 관계되는 동작의 실행시에 상기 호스트 마이크로 프로세서에 의해 사용되는 제2타입의 프로그램 정보를 저장하며 상기 블럭들의 제4그룹 중 다른 하나와 관계된 각 저장위치의 상기 제3액세스 제어 비트 위치는 시스템의 완전성을 위해 상기 애플리케이션 마이크로 프로세서에 의해 상기 블럭들의 제4그룹내의 저장 위치들로의 액세스를 금지하도록 하기 위한 상기 제2상태로 세트되며 상기 각 저장 위치의 상기 제4액세스 제어 비트 위치는 상기 호스트 마이크로 프로세서에 의해 제4그룹의 위치들내의 저장위치들로 액세스를 인에이블하도록 하기 위한 상기 제1상태로 세트되는 애프리케이션 카드.

청구항 13. 제12항에 있어서, 상기 블럭들의 제1, 제2, 제3 및 제4그룹들은 다른 갯수의 블럭들을 포함하는 애플리케이션 카드.

청구항 14. 제1항에 있어서, 상기 애플리케이션 카드는 상기 특정 애플리케이션을 실행하기 위한 동작을 실행하도록 프로그램된 애플리케이션 마이크로 프로세서를 더 포함하며, 상기 애플리케이션 마이크로 프로세서는 상기 내부 버스의 상기 어드레스, 데이터 및 제어부에 결합되며 메모리 액세스가 이루어지는 상기 타입을 한정하는 신호들을 발생시키는 애플리케이션 카드.

청구항 15. 제1항에 있어서, 상기 액세스 제어 마이크로 프로세서는 파워 온 신호에 응답하여 상기 특정 애플리케이션의 실행시에 사용되는 상기 비 휘발성 메모리 매핑 정보를 상기 액세스 식별 논리 유닛에 로드 하는 애플리케이션 카드.

청구항 16. 제1항에 있어서, 상기 특정 애플리케이션의 실행중에, 상기 액세스 제어 마이크로 프로세서는 상기 호스트 마이크로 프로세서로부터 수신된 상기 액세스 식별 논리 유닛내에 저장된 상기 비 휘발성 메모리 매핑 정보를 변경시키기 위한 각 요청에 응답하여서만 상기 호스트 마이크로 프로세서에 의해 성공적인 증명동작이 실행된 후에 상기 비 휘발성 메모리 매핑 정보를 변경시키는 애플리케이션 카드.

청구항 17. 제16항에 있어서, 상기 액세스 제어 마이크로 프로세서의 비 휘발성 메모리 구성정보는 상기 증명 동작 실행시에 상기 액세스 제어 마이크로 프로세서에 의해 사용되는 다수의 패스워드를 더 포함하는 애플리케이션 카드.

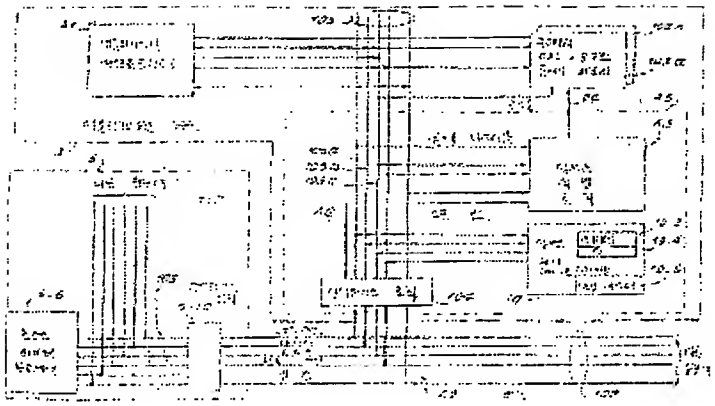
청구항 18. 버스 인터페이스를 통해 결합된 호스트 마이크로 프로세서와 조합되어 사용되는 애플리케이션 카드로서; 상기 호스트 마이크로 프로세서로의 그리고 그 호스트 마이크로 프로세서로부터의, 어드레스, 데이터 및 제어 정보를 포함하는 요청들을 송수신하도록 상기 버스 인터페이스에 유효하게 결합된 인터페이스 논리회로 수단; 상기 인터페이스 논리회로 수단에서의 신호를 포함하는 상기 요청을 전달하도록 어드레스, 데이터 및 제어부를 갖는 내부버스; 상기 내부 버스에 접속되며, 특정 애플리케이션을 실행하도록 코드된 비 휘발성 메모리 매핑 정보를 포함하는 구성 정보를 저장하는 어드레스 가능한 비 휘발성 메모리를 포함하는 액세스 제어 마이크로 프로세서; 상기 애플리케이션 마이크로 프로세서는 상기 내부 버스의 상기 어드레서, 데이터 및 제어정보를 수신하기 위해 상기 마이크로 프로세서와 공통으로 상기 내부 버스에 접속되며, 상기 애플라케이션을 실행하기 위해 요구되는 별개의 액세스 타입 정보를 저장하기 위한 복수의 저장위치들으로 가진 다수의 블럭들로 구성되며, 상기 블럭들이 다수의 블럭들의 그룹들을 가지며, 상기 각 그룹이 상기 특정 애플리케이션의 실행시에 상기 호스트 및 애플리케이션 마이크로 프로세서들에 의해 사용되는 다른 데이터 및 프로그램 정보를 저장하도록 하기 위한 적어도 하나의 어드레스가 가능한 비 휘발성 메모리; 및 상기 내부 버스의 어드레스, 데이터 및 제어부 및 상기 비 휘발성 메모리에 결합되는 액세스 식별 논리 유닛으로서,상기 애플리케이션 실행에 관계된 상기 애플리케이션 및 호스트 마이크로 프로세서 및 메모리 요청에 응답하는 상기 액세스 식별 논리 유닛에 의해 각 블럭에 저장된 상기 데이터 또는 프로그램 정보중에 하나에 대해 만들어지는 별개의 메모리 액세스 타입을 한정하도록 코드된 상기 갯수의 블럭들의 상기 갯수의 그룹들의 상기 비 휘발성 메모리 매핑 정보에 대응하는 액세스 바이 타입 정보를 저장하고, 상기 마이크로 프로세서가 상기 액세스 바이 타입 정보에 의해 한정된 상기 메모리 요청만을 만드는 것에 의해 상기 블럭에 저장된 정보에 액세스를 인에이블하도록 하기 위한 상기 메모리 요청의 상기 어드레스 정보에 의해 지정된 상기 블럭들 중 하나의 상기 액세스 바이타입 정보를 판독하는 액세스 식별 논리 유닛을 포함하는 애플리케이션 카드.

청구항 19. 제1항에 있어서, 상기 액세스 식별 논리 유닛은; 상기 내부 버스의 어드레스, 데이터 및 제어부에 각각 접속된 어드레스, 데이터 및 제어입력, 상기 비 휘발성 메모리에 접속된 출력, 및 상기 비 휘발성 메모리 매핑 정보를 저장하기 위한 상기 다수의 블럭들의 갯수에 대응하는 다수의 저장 위치들을 가진 랜덤 액세스 메모리(RM) 어레이를 포함하며, 각 저장 위치는 상기 갯수의 블럭들내의 상기 갯수의 그룹들에 대응하는 다수의 액세스 제어 비트 위치들을 가지며, 상기 액세스 제어 비트 위치들은 상기 특정 애플리케이션 실행을 위하여 사익 애플리케이션 및 호스트 마이크로 프로세서에 의해 요구되는 메모리 액세스 타입을 지정하기 위한 상기 메모리 매핑 정보에 의해 한정되는 소정 상태로 세트되며, 상기 RAM 어레이는 각 메모리 요청에 응답하여 상기 어드레스 정보에 의해 지정된 상기 다수의 저장 위치들 중 하나에서의 메모리 매핑 정보를 판독하고, 상기 인터페이스 로직 회로 수단으로부터 상기 신호들에 의해 한정된 상기 액세스 제어 비트 위치중의 하나로부터 상기 소정 상태중 하나로 대표되는 제어 신호는 상기 소정 상태들중 하나에 의해 한정되어서만 상기 액세스를 인에이블링 하도록 하기 위한 메모리 액세스 타입 및 메모리 액세스 요청으로서의 상기 애플리케이션 또는 호스트 마이크로 프로세서를 지정하는 애플리케이션 카드.

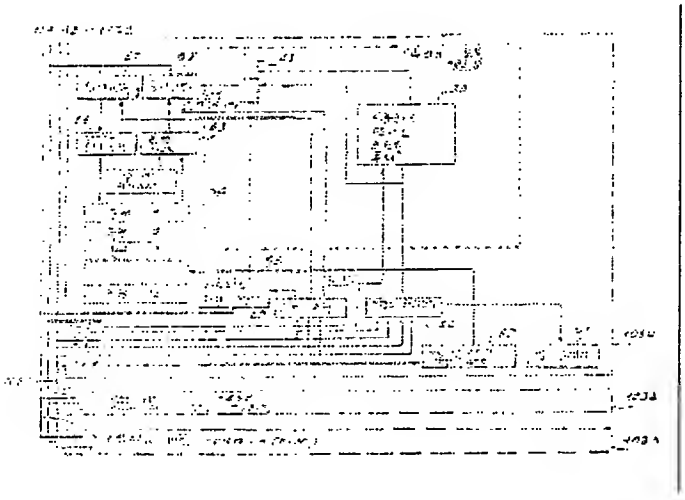
※ 참고사항 : 최초출원 내용에 의하여 공개하는 것임.

도면

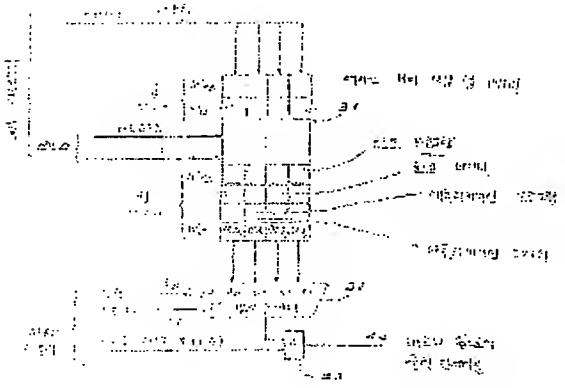
도면1



도면2



도면3



This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.